

REMARKS

The Office Action mailed July 30, 2003 has been carefully considered. Applicants request that the Examiner consider the following remarks, and then pass the application to allowance.

Information Disclosure Statement

Applicant gratefully acknowledges the Examiners review and initialing of PTO-1449. However, the foreign patent documents were not initialed and/or considered by the Examiner. In order to have a complete record, Applicant respectfully requests the Examiner to consider the references and then initial and return the completed PTO-1449. A copy of the previously filed PTO-1449 is enclosed for the Examiner's convenience.

Changes in the Specification

By the present Amendment, the Specification has been amended to correct typographical errors found during a review of the application. No new matter has been added.

Pending Claims

Claims 1-4 are pending.

Art Rejection

In the Office Action, claims 1-4 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shi et al (U.S. Pat. No. 5,875,296) in view of Applicant's admitted prior art (APA). Specifically, the rejection relied on Shi for disclosing an HTTP path name, a client, and identity, and identity of data, a container, an X module manager, data identified and a subsequent transmission. The rejection relied APA for teaching that the X module is an administrative module and it would have been obvious to apply the teaching of APA to Shi in order to provide an access page to stream servers.

Applicant respectfully submits that Shi does not teach the limitations as suggested by the rejection. As understood, Shi discloses a method for authenticating a user to a web server having a distributed file system. The method provides a security mechanism using a web server with distributed file services. More specifically, as seen in step 68 of Figure 4, Shi discloses the web server sending a login HTML form and a cookie to the browser of the client (i.e., user). The cookie is an Internet mechanism that can be used to both store and retrieve information on the client side of the connection. (Shi, Col. 6, lines 51-53). In step 70, the user fills in the user ID and password, and in step 72 the client returns the completed form and cookie to the server. The DCE_LOGIN is run in step 74 wherein a credential is generated by the server for use by the client from the password and user ID. An unique ID (DCE UUID) for the user is created in step 77. In step 78, the credential is stored in a database associated with the session manager and indexed using the unique ID. In steps 82 and 83, the server sends a new cookie to the browser which includes the unique

ID created in step 76 and the cookie created in step 68 is destroyed. The unique ID is a secret handle that is an entry into a table of credentials stored from step 78. On subsequent requests for service by the client, the client transmits the new cookie containing the unique ID which is used as a pointer to the user's DFS credentials stored in the database.

Applicant respectfully submits that Shi does not teach or suggest accessing internal server data using HTTP commands. For example, as recited in claim 2, the claimed invention is a method for obtaining internal server data locally or remotely across a computer network. The method comprises processing at a network server an HTTP path name generated at a client wherein the HTTP path name includes an identity container within the server and an identity of internal server data maintained with the container. The method further includes an administrative module of the server that processes the path name to generate the internal server data identified in the path name for subsequent transmission to the client. Finally, the internal server data is transmitted to the client. In this regard, the HTTP path name can be used to access internal server data easily for analysis.

Claims 1 - 4 are not anticipated or rendered obvious in view of Shi because Shi does not teach or suggest using an HTTP path name to access internal server data of the server. As understood, Shi discloses a client transmitting either a cookie and/or a login form in order to authenticate with the server. Shi does not disclose sending an HTTP path name having an identity of internal server data maintained with said container in order to access the internal server data. As described by claims 1-4, the present invention is directed toward accessing internal server data using HTTP path names. On the other hand, as

previously discussed, Shi discloses accessing password and credential information stored on the server by transmitting either a cookie, or password and ID information. There is no teaching or suggestion within Shi for using HTTP path names to access internal server data. Shi discloses using cookies for storing and retrieving information on the client side of the connection, but not for accessing internal server data. Accordingly, claims 1 - 4 are not rendered obvious in view of the Shi reference because neither Shi nor APA discloses accessing internal server data using the HTTP path name.

Conclusion

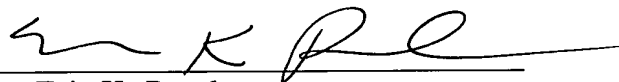
In view of the preceding discussion, Applicant respectfully urges that the claims of the present application define patentable subject matter and should be passed to allowance. Such allowance is respectfully solicited.

If the Examiner believes that a telephone call would help advance prosecution of the present invention, the Examiner is kindly invited to call the undersigned attorney at (650) 622-2300.

Respectfully submitted,

Date: September 18, 2003

By: _____



Eric K. Proul

Registration No. 45,025

P. O. Box 1404
Alexandria, Virginia 22313-1404
(650) 622-2300